

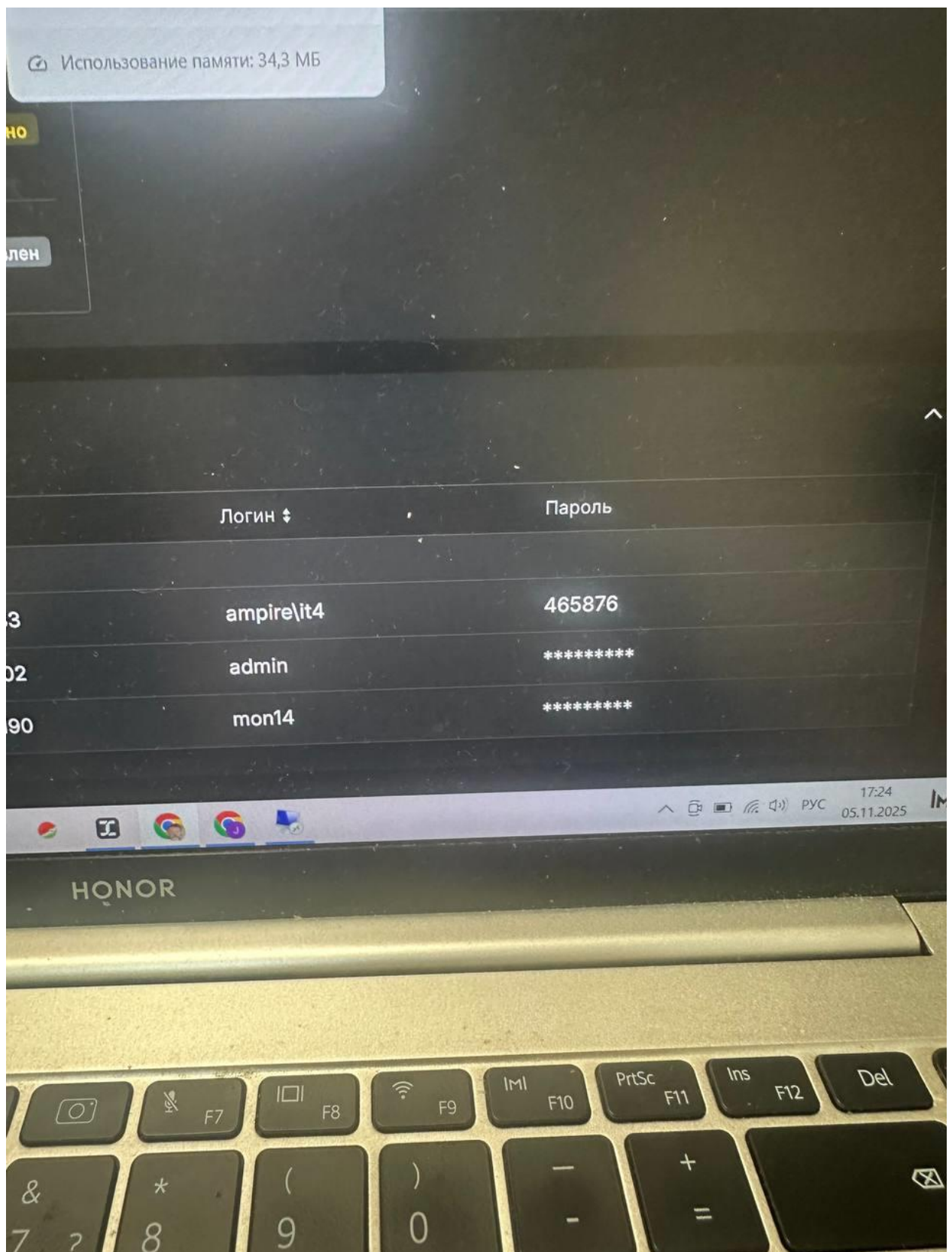
Козлова Нонна, Пинега Белла, Световидова Полина, Лазева Диана, Салькова Кристина

Лабораторная работа #2

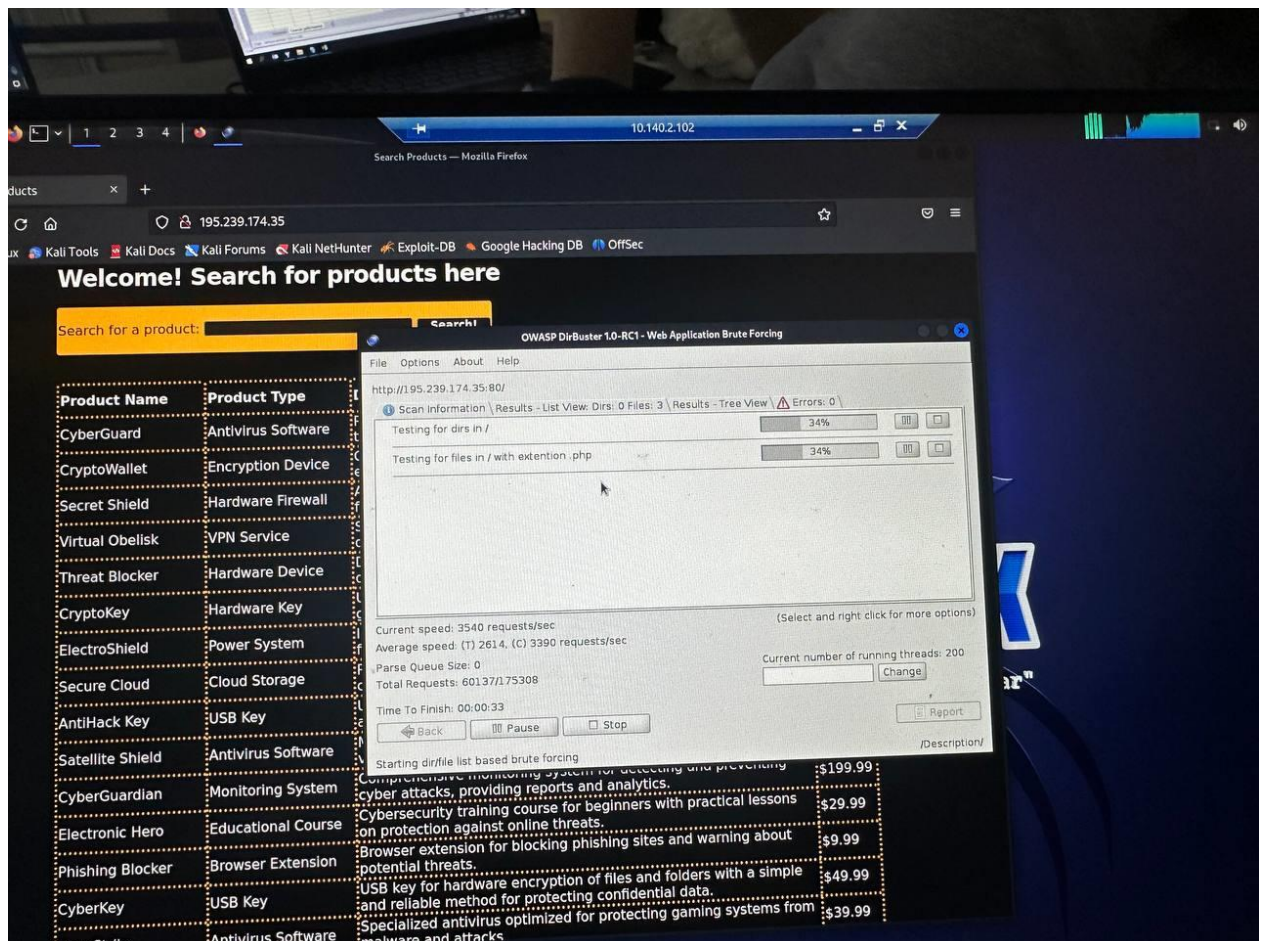
Необходимо найти в директориях сайта два флага, прочитать их значения и передать на портал

Получение первого флага

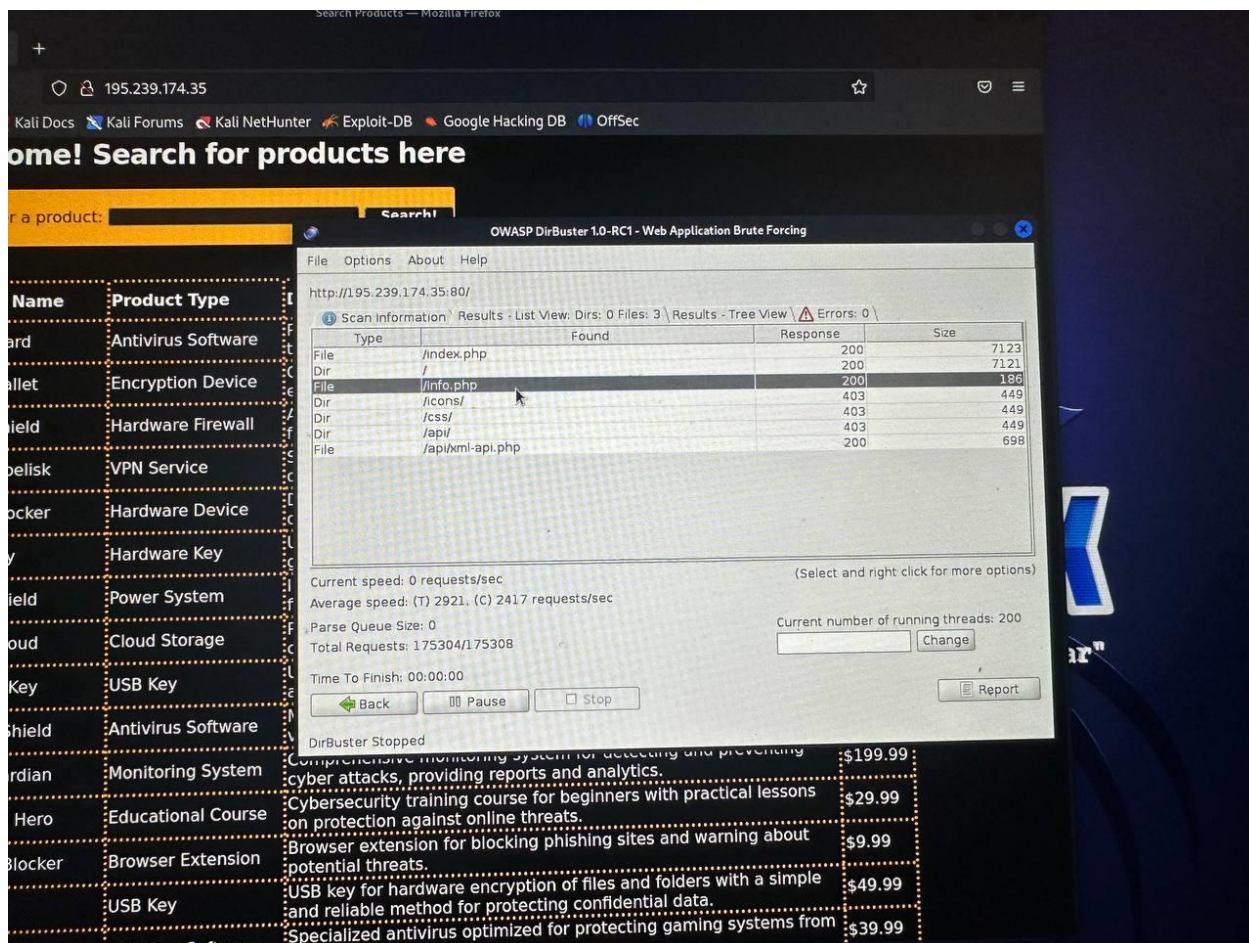
- Запускаем удаленный рабочий стол



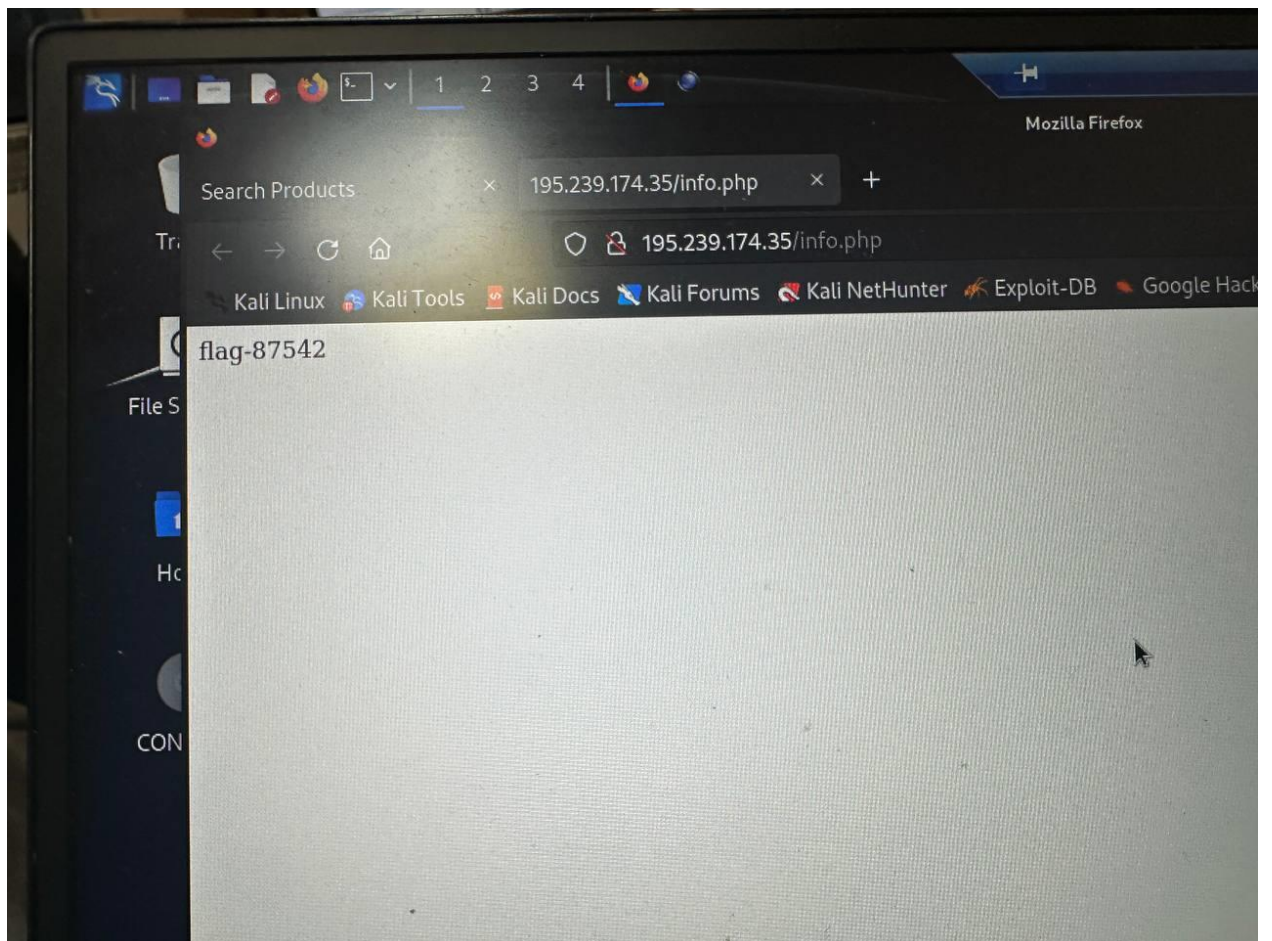
- Запускаем DirBuster и указываем <http://195.239.174.35/>, выбираем словарь и отключаем опцию Be Recursive.



- Для получения флага переходим по ссылке <http://195.239.174.35/info.php> из контекстного меню DirBuster

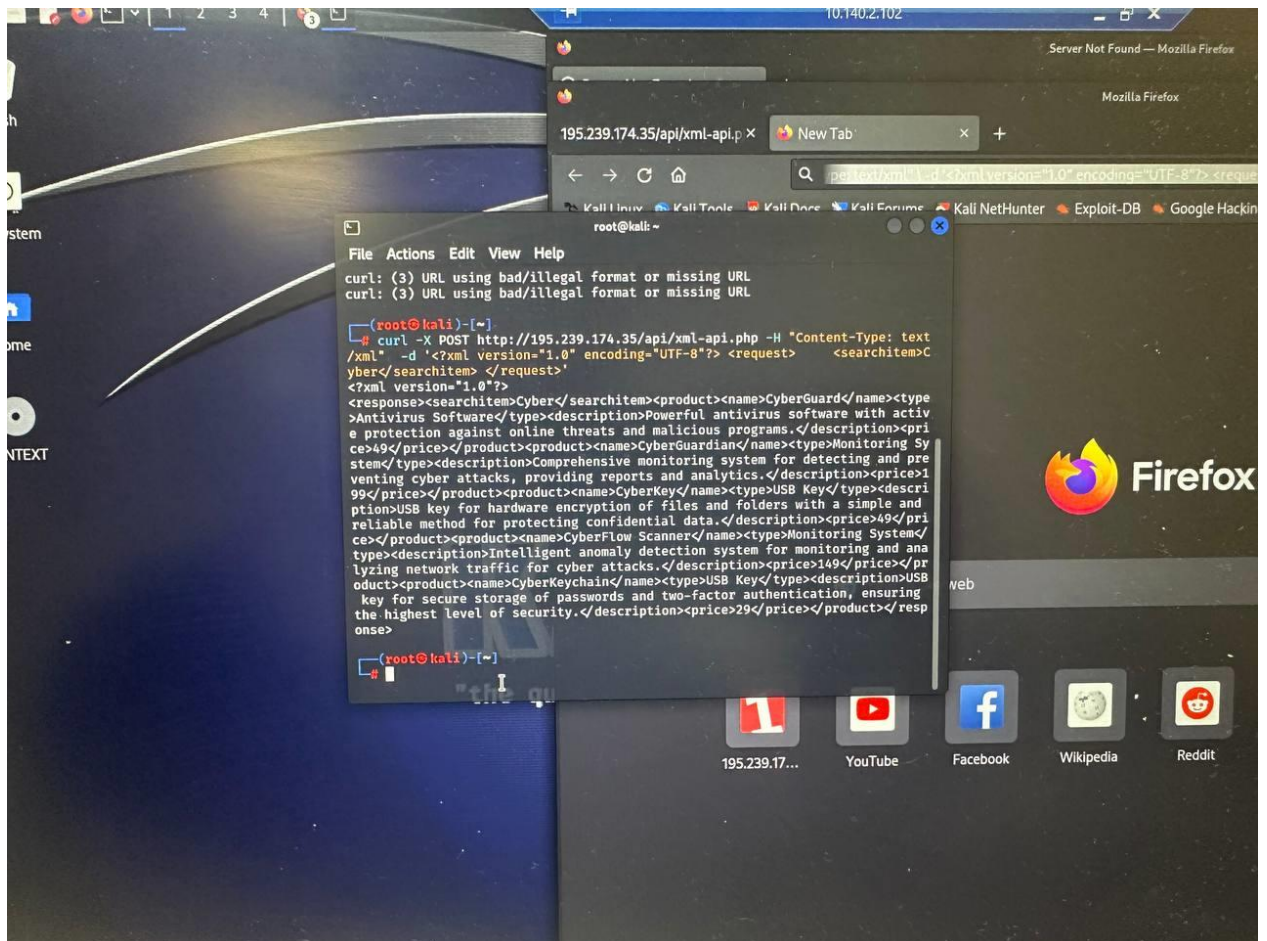


- Получение флага «Исследование веб-директорий магазина»

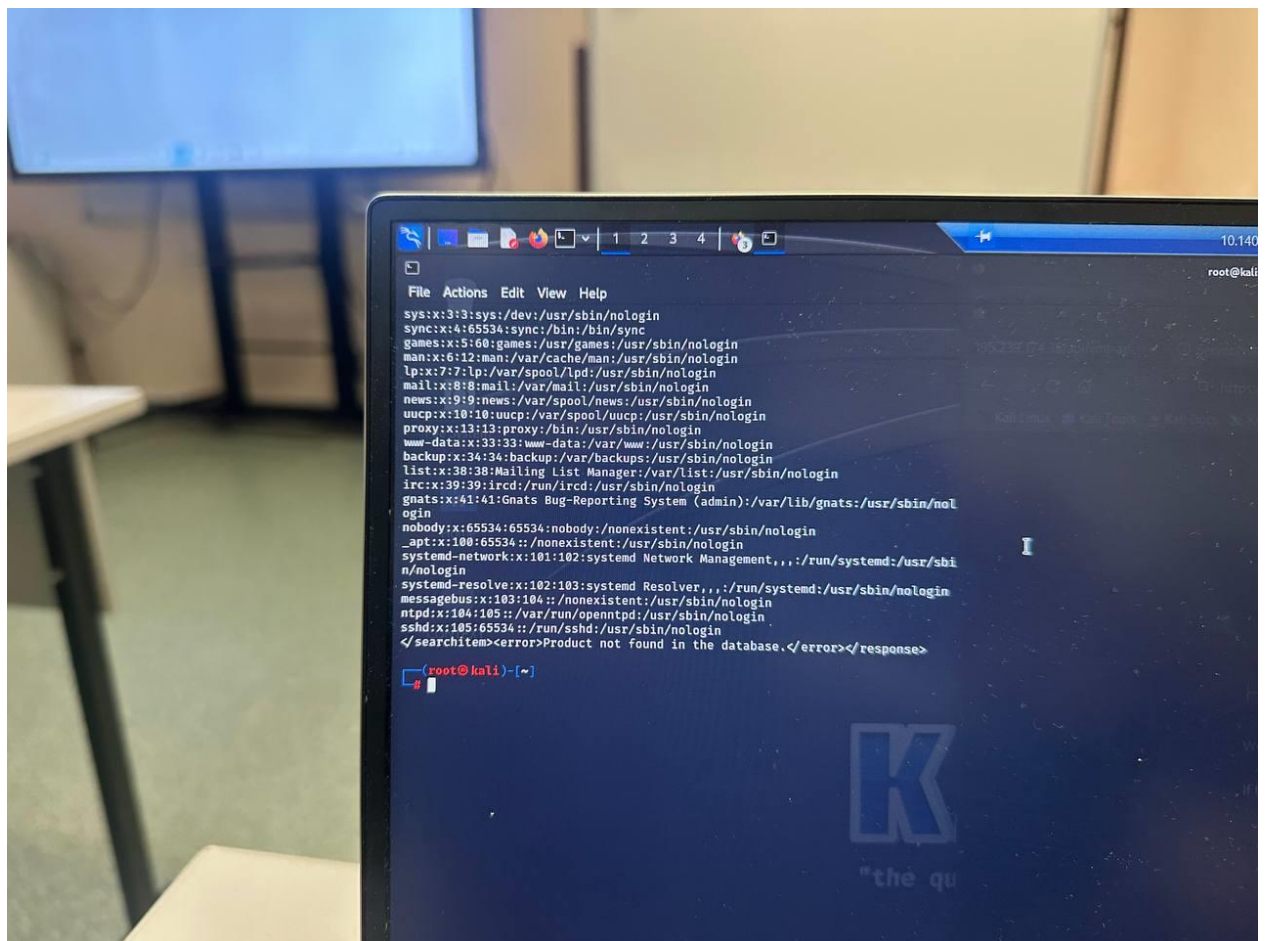


Получение второго флага

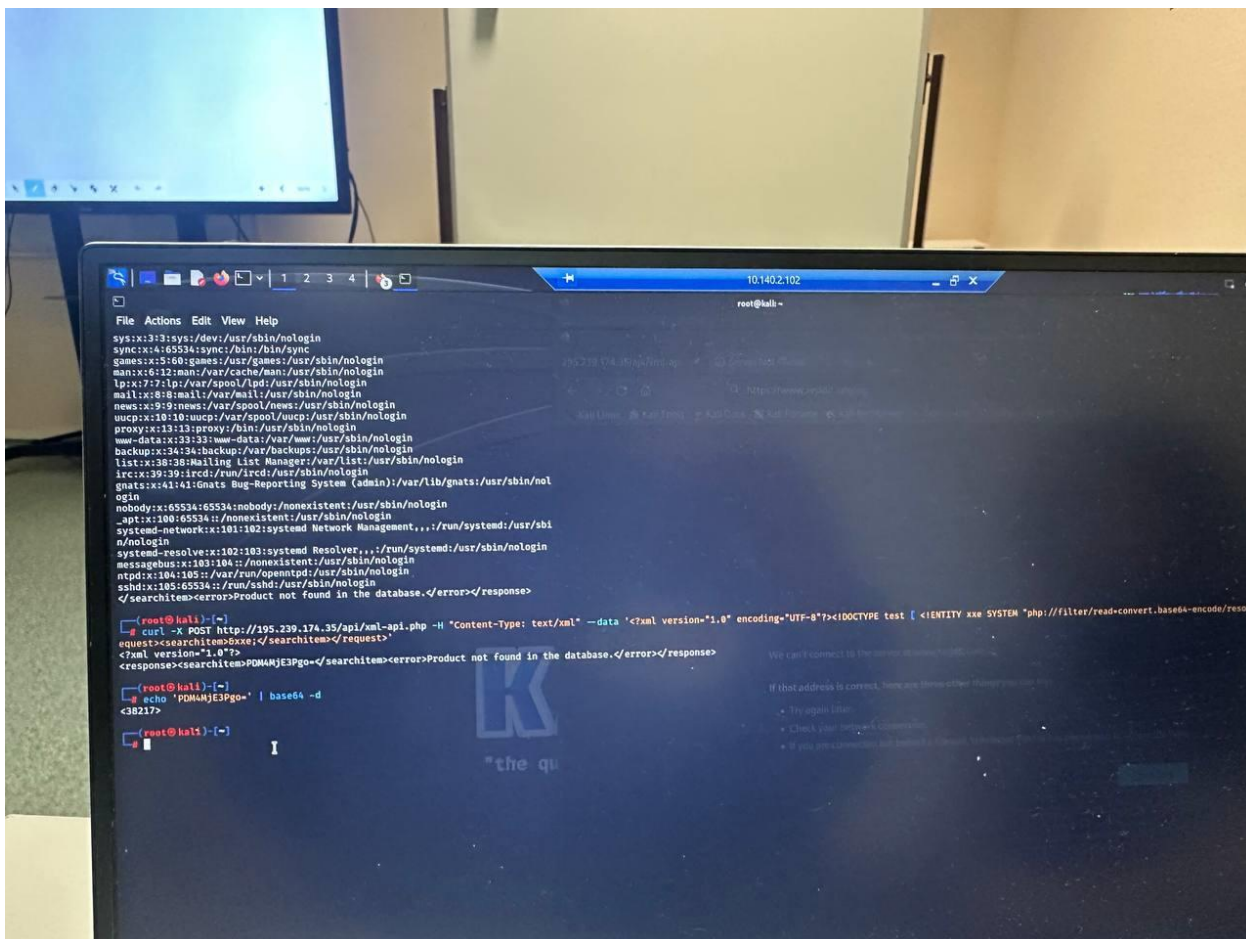
- Открываем внешний вид страницы API и делаем запрос



- Результат обработки



- Получение второго флага



Получение сессии с веб-ресурсом посредством XXE

- Используем уязвимость XXE и обёртку exptest:// для выполнения команд на сервере.
- Генерируем RHP-полезную нагрузку для обратного подключения с помощью msfvenom.
- Запускаем на своей машине HTTP-сервер для раздачи payload.
- Используем XXE-запрос с curl для загрузки payload на целевой сервер.
- Запускаем в Metasploit обработчик multi/handler для приёма соединения.

